I CLAIM

1. A data processing apparatus, comprising:

a processor operable in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain, said processor being operable such that when executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode;

a memory unit comprising a plurality of entries and operable to store data required by the processor, each entry being operable to store one or more data items consisting of either secure data or non-secure data, and a flag being associated with each entry in the memory unit to store a value indicating whether the one or more data items stored in the associated entry are said secure data or said non-secure data;

when the processor is operating in said at least one non-secure mode, the memory unit being operable, upon receipt of a memory access request issued by the processor when access to an item of data is required, to prevent access to any data item within an entry of the memory unit that the associated flag indicates has secure data stored therein.

2. A data processing apparatus as claimed in Claim 1, wherein the memory unit is a cache, and each said entry is a cache line of the cache.

3. A data processing apparatus as claimed in Claim 1, wherein the memory unit is coupled to the processor via a processor bus, the memory unit and processor forming a device, and the data processing apparatus further comprises a device bus via which the device is connectable to a further memory unit, the further memory unit having secure memory for storing secure data and non-secure memory for storing non-secure data.

4. A data processing apparatus as claimed in Claim 3, wherein if the memory access request specifies a data item that is not stored within the memory unit, the memory access

request is output on to the device bus to cause that data item to be accessed in the further memory unit, the data processing apparatus further comprising:

partition checking logic connected to the device bus and operable, whenever the memory access request is issued by the processor when operating in said at least one non-secure mode and is output onto the device bus, to detect if the memory access request is seeking to access the secure memory of the further memory unit, and upon such detection to prevent the access specified by that memory access request.

5. A data processing apparatus as claimed in Claim 4, wherein if the memory access request specifies a data item that is not stored within the memory unit, then if the partition checking logic determines that the processor is allowed to access that data item, that data item is retrieved from the further memory unit and stored in one of said entries of the memory unit, the value to be set for the flag associated with that entry being indicated by the partition checking logic.

6. A data processing apparatus as claimed in Claim 3, wherein the further memory unit is a main memory of the data processing apparatus.

7. A data processing apparatus as claimed in Claim 1, wherein the flag is contained within the memory unit and comprises a single bit set to indicate whether the associated entry has secure data or non-secure data stored therein.

8. A data processing apparatus as claimed in Claim 1, wherein the memory unit is operable to issue an abort signal if the processor, whilst operating in said at least one non-secure mode, seeks to access any data item within an entry of the memory unit that the associated flag indicates has secure data stored therein.

9. A data processing apparatus as claimed in Claim 1, wherein the processor is coupled to the memory unit via a memory management unit operable, upon receipt of the memory access request, to perform one or more predetermined access control functions to control issuance of the memory access request to the memory unit.

10. A data processing apparatus as claimed in Claim 9, wherein the memory access request specifies a virtual address, and one of said predetermined access control functions comprises conversion of the virtual address to a physical address.

11. A method of controlling access to a memory unit of a data processing apparatus, the data processing apparatus comprising a processor operable in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain, said processor being operable such that when executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode, the data processing apparatus further comprising a memory unit comprising a plurality of entries and operable to store data required by the processor, each entry being operable to store one or more data items consisting of either secure data or non-secure data, the method comprising the steps of:

associating a flag with each entry in the memory unit;

when said one or more data items are stored in an entry of the memory unit, storing a value within the associated flag indicating whether said one or more data items are said secure data or said non-secure data;

when the processor is operating in said at least one non-secure mode, and upon receipt of a memory access request issued by the processor when access to an item of data is required, preventing access to any data item within an entry of the memory unit that the associated flag indicates has secure data stored therein.

12. A method as claimed in Claim 11, wherein the memory unit is a cache, and each said entry is a cache line of the cache.

13. A method as claimed in Claim 11, wherein the memory unit is coupled to the processor via a processor bus, the memory unit and processor forming a device, and the method further comprises the step of:

connecting the device to a further memory unit via a device bus, the further memory unit having secure memory for storing secure data and non-secure memory for storing non-secure data.

14. A method as claimed in Claim 13, wherein if the memory access request specifies a data item that is not stored within the memory unit, the method further comprises the steps of:

outputting the memory access request on to the device bus to cause that data item to be accessed in the further memory unit;

whenever the memory access request is issued by the processor when operating in said at least one non-secure mode and is output onto the device bus, employing partition checking logic to detect if the memory access request is seeking to access the secure memory of the further memory unit, and upon such detection to prevent the access specified by that memory access request.

15. A method as claimed in Claim 14, wherein if the memory access request specifies a data item that is not stored within the memory unit, the method further comprises the steps of:

employing the partition checking logic to determine whether the processor is allowed to access that data item; and if so

retrieving that data item from the further memory unit and storing that data item in one of said entries of the memory unit; and

employing the partition checking logic to determine the value to be set for the flag associated with that entry.

16. A method as claimed in Claim 13, wherein the further memory unit is a main memory of the data processing apparatus.

17. A method as claimed in Claim 11, wherein the flag is contained within the memory unit and comprises a single bit set to indicate whether the associated entry has secure data or non-secure data stored therein.

18. A method as claimed in Claim 11, wherein the memory unit is operable to issue an abort signal if the processor, whilst operating in said at least one non-secure mode, seeks to access any data item within an entry of the memory unit that the associated flag indicates has secure data stored therein.

19. A method as claimed in Claim 11, wherein the processor is coupled to the memory unit via a memory management unit operable, upon receipt of the memory access request, to perform one or more predetermined access control functions to control issuance of the memory access request to the memory unit.

20. A method as claimed in Claim 19, wherein the memory access request specifies a virtual address, and one of said predetermined access control functions comprises conversion of the virtual address to a physical address.